

(51) Int.Cl. ⁷	識別記号	F I	ページコード ⁸ (参考)
G 0 6 F 3/06	3 0 1	C 0 6 F 3/06	3 0 1 J 5 B 0 6 J
	3 0 4		3 0 4 H
	5 4 0		5 4 0

審査請求 未請求 請求項の数14 O L (全 13 頁)

(21) 出願番号	特願2002-326263 (P2002-326263)	(71) 出願人	000005108 株式会社日立製作所 東京都千代田区神田駿河台四丁目 6 番地
(22) 出願日	平成14年11月11日 (2002.11.11)	(72) 発明者	内山 靖文 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内
(31) 優先権主張番号	特願2002-63646 (P2002-63646)	(72) 発明者	増田 晴樹 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内
(32) 優先日	平成14年3月8日 (2002.3.8)	(74) 代理人	100075096 弁理士 作田 康夫
(33) 優先権主張国	日本 (J P)		

最終頁に続く

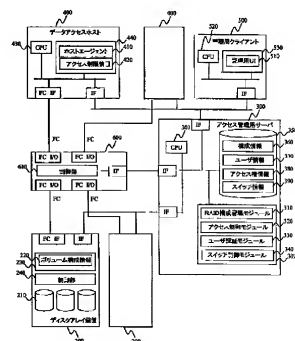
(54) 【発明の名称】 アクセス管理用サーバ、ディスクレイシステム、及びそのアクセス管理方法

(57) 【要約】

【課題】 記憶領域の割当て、その記憶領域に対するアクセス権限の設定を容易に行う。

【解決手段】 複数のディスク装置に対するユーザからのアクセスを管理するのであって、管理用クライアントにて各ユーザ I D ごとに論理ボリュームの構成情報の変更権限を設定し、アクセス管理用サーバにユーザ情報、アクセス権情報として保存する。アクセス管理用サーバは、保存されたユーザ情報、アクセス権情報に基づいてディスクレイ装置のボリューム構成情報を生成し、ディスクレイ装置に設定する。

図 11



【特許請求の範囲】

【請求項1】 複数のディスク装置に対するアクセスを管理するアクセス管理用サーバであって、前記各ディスク装置が記憶する論理的に分割された論理ボリュームの情報と、ユーザの識別子毎に論理ボリュームに対するアクセス権の設定を許可する情報とが記憶された記憶装置から、送られてきたユーザの識別子に基づいてアクセス権の設定が許可された論理ボリュームに関する情報を送ることを特徴とするアクセス管理用サーバ。

【請求項2】 請求項1に記載されたアクセス管理用サーバにおいて、送られてきた論理ボリュームに対するアクセス権の情報から論理ボリュームとホストアドレスとを対応づけた構成定義情報を生成し、生成された構成定義情報を当該論理ボリュームに対応する物理ディスクが存在するディスク装置へ送ることを特徴とするアクセス管理用サーバ。

【請求項3】 複数のディスク装置に対するユーザからのアクセスを管理するアクセス管理用サーバであって、前記各ディスク装置が記憶する論理的に分割された論理ボリュームについて各ユーザの識別子毎に定義されたアクセス権の情報を有し、前記論理ボリュームに対する前記アクセスの要求を受けるとユーザの識別子と前記アクセス権の情報に基づき、前記アクセスに対して許可あるいは不許可いずれかの判断を行うアクセス制御手段を備えたことを特徴とするアクセス管理用サーバ。

【請求項4】 前記アクセスは、前記論理ボリュームの定義を設定するためのアクセスであって、前記アクセス権の情報は、前記アクセスの対象である前記論理ボリュームの定義の設定について許可あるいは不許可のいずれかを示す論理ボリューム定義設定権限情報を含んでおり、前記アクセス制御手段は、前記論理ボリューム定義設定権限情報に基づき、前記論理ボリュームの定義の設定を許可あるいは不許可とすることを特徴とする請求項3に記載のアクセス管理用サーバ。

【請求項5】 前記アクセス制御手段による、前記論理ボリュームの定義の設定を許可あるいは不許可とする判断の結果に応じ、該設定を実行する論理ボリューム定義設定実行手段を備えることを特徴とする請求項4に記載のアクセス管理用サーバ。

【請求項6】 前記アクセスは、前記論理ボリュームのデータに対するアクセスであって、前記アクセス制御手段の判断の結果に基づき、前記アクセスの要求に対して該アクセスを可能とするパス制御手段を備えたことを特徴とする請求項3に記載のアクセス管理用サーバ。

【請求項7】 複数のディスク装置を有するディスクアレイ装置と、前記ディスクアレイ装置に対するユーザか

らのアクセスを管理するアクセス管理用サーバとを備えたディスクアレイシステムであって、前記アクセス管理用サーバは、

前記各ディスク装置が記憶する各論理ボリュームについて各ユーザの識別子毎に定義されたアクセス権の情報を有し、前記論理ボリュームに対する前記アクセスの要求を受けると、前記ユーザの識別子と前記アクセス権の情報に基づき、前記アクセスに対して許可あるいは不許可いずれかの判断を行うアクセス制御手段を備えた、ことを特徴とするディスクアレイシステム。

【請求項8】 前記アクセスは、前記論理ボリュームの定義を設定するためのアクセスであって、前記アクセス権の情報は、前記アクセスの対象である前記論理ボリュームの定義の設定について許可あるいは不許可のいずれかを示す論理ボリューム定義設定権限情報を含んでおり、

前記アクセス制御手段は、前記論理ボリューム定義設定権限情報に基づき、前記論理ボリュームの定義の設定を許可あるいは不許可とすることを特徴とする請求項7に記載のディスクアレイシステム。

【請求項9】 前記アクセス制御手段による、前記論理ボリュームの定義の設定を許可あるいは不許可とする判断の結果に応じ、該設定を実行する論理ボリューム定義設定実行手段を備えることを特徴とする請求項8に記載のディスクアレイシステム。

【請求項10】 前記アクセスは、前記論理ボリュームのデータに対するアクセスであって、前記アクセス制御手段の判断の結果に基づき、前記アクセスの要求に対して該アクセスを可能とするパス制御手段を備えたことを特徴とする請求項7に記載のディスクアレイシステム。

【請求項11】 複数のディスク装置に対するユーザからのアクセスを管理する方法であって、前記各ユーザから前記論理ボリュームに対する前記アクセスの要求を受けると、前記各ディスク装置が記憶する各論理ボリュームについて各ユーザの識別子毎に定義されたアクセス権の情報に基づき、前記アクセスに対して許可あるいは不許可いずれかの判断を行うことを特徴とするアクセス管理方法。

【請求項12】 前記アクセスは、前記論理ボリュームの定義を設定するためのアクセスであって、前記アクセス権の情報は、前記アクセスの対象である前記論理ボリュームの定義の設定について許可あるいは不許可のいずれかを示す論理ボリューム定義設定権限情報を含んでおり、

前記論理ボリューム定義設定権限情報に基づき、前記論理ボリュームの定義の設定を許可あるいは不許可とすることを特徴とする請求項11に記載のアクセス管理方法。

【請求項13】 前記論理ボリュームの定義の設定を許可あるいは不許可とする判断の結果に応じ、該設定を実行することを特徴とする請求項12に記載のアクセス管理方法。

【請求項14】 複数のディスク装置に対するアクセスを管理する方法であって、

送られてきたユーザの識別子に基づいて、当該ユーザの識別子に対してアクセス権の設定が許可された論理ボリュームの情報を特定し、
前記特定された論理ボリュームに対して、アクセス権の設定が可能なユーザの識別子を設定することを特徴とするアクセス管理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、アクセス管理用サーバ、ディスクアレイシステム、及びそのアクセス管理方法に関する。

【0002】

【従来の技術】近年、企業などで利用される計算機システムで扱われる情報量は、飛躍的に増大しており、これに伴いデータを記憶するディスク装置などの容量も増加の一途をたどっている。例えば、磁気ディスク装置においては、数TB（テラバイト）の容量を持つ装置も珍しくなくなっている。このようなディスク装置に関して、例えば、特許文獻1などには、1台の記憶制御装置が管理している論理ディスク装置の再配置について開示されている。具体的には、アクセス情報に基づく保守員の判断により、アクセス頻度の高い論理ディスク装置をより高速な物理ディスク装置へ再配置し、シーケンシャルアクセスの比率の高い論理ディスク装置をよりシーケンシャルアクセス性能の高い物理ディスク装置へ再配置することが開示されている。

【特許文獻1】特開平9-274544号公報

【0003】

【発明が解決しようとする課題】上記従来技術では、ユーザ単位あるいはホスト単位に記憶装置を割当てることについては記載されていない。

【0004】つまり、記憶装置の容量が増加すると、その記憶装置を有効に利用するために複数のユーザによって共有することが考えられる。また、SSP(Storage Service Provider)等において、記憶装置をいくつかの区分に分けて利用するようなサービスを行うことが考えられる。このような場合、管理者はユーザ単位あるいはホスト単位に記憶装置の領域を割当てる必要がある。更に、ある領域を割当られたユーザは、その領域を有効に利用するために他のユーザが利用できるようにする必要がある。

【0005】本発明は、このような課題に鑑みてなされたもので、ユーザ単位あるいはホスト単位に対して記憶領域を割当て、更にユーザ単位あるいはホスト単位にその記憶領域に

対するアクセス権限を設定可能な方法又は装置を提供することを目的とする。

【0006】

【課題を解決するための手段】前記目的を達成すべく、本発明の主たる発明では、複数のディスク装置に対するユーザからのアクセスを管理するのであって、前記各ユーザから前記論理ボリュームに対する前記アクセスの要求を受けると、前記各ディスク装置が記憶する各論理ボリュームについて各ユーザ毎に定義されたアクセス権の情報に基づき、前記アクセスに対して許可あるいは不許可いすれかの判断を行う。

【0007】

【発明の実施の形態】本発明の実施の形態に係るアクセス管理用サーバ、ディスクアレイシステム、及びそのアクセス管理方法につき、図面を参照して説明する。図1は、システム全体のブロック図を示したものであり、複数のデータアクセスホスト400、管理用クライアント500、アクセス管理用サーバ300、複数のディスクアレイ装置200、スイッチ600とを有している。データアクセスホスト400、管理用クライアント500、アクセス管理用サーバ300、ディスクアレイ装置200、スイッチ600は、例えばIPプロトコルによるネットワークによって接続されている。また、データホスト400、スイッチ600、ディスクアレイ200は、ファイバチャネルプロトコルによるネットワークに接続されている。尚、図1においてIPプロトコルのネットワークとのインタフェースを「IF」、ファイバチャネルプロトコルによるネットワークとのインタフェースを「FC IF」として示している。また、ディスクアレイ装置200と、アクセス管理用サーバ300によって構成されたシステムをディスクアレイシステムと称す。

【0008】ディスクアレイ装置200は、RAID (Redundant Array for Inexpensive Disk) 装置で構成される。アクセス管理用サーバ300は、ディスクアレイ装置200に対するユーザからのアクセスを管理する。

【0009】データアクセスホスト400は、ディスクアレイ装置200の論理ボリュームを利用するサーバ機であり、メモリ440と、メモリに格納されたプログラムを実行するCPU430とを有している。メモリ440には、ホストエージェント410のプログラムと、アクセス制限情報420が格納されている。

【0010】管理用クライアントコンピュータ500は、メモリ530と、メモリ530に格納されたプログラムを実行するCPU520とを有している。また、メモリ530には管理用UI (User Interface、コンソール) 510のプログラムが格納されている。この管理用UI 510は、ユーザ（ストレージ管理者）が入力するID等の情報をアクセス管理用サーバ300へ通知す

る。管理用クライアントコンピュータ500は、ユーザ（ストレージ管理者）の管理用UI510を通じた操作入力に基づき、論理ボリュームの構成を定義したり、ユーザのアクセス権を設定する。

【0011】ディスクアレイ装置200を構成するRAID装置は、一又は複数のボリュームを論理的な記憶領域としてデータアクセスホスト400に提供する機能を有するディスクストレージ装置である。ディスクアレイ装置200は、複数のディスク装置210、制御部240、メモリ230とを有している。また、メモリ230には論理ボリュームの構成が定義されたボリューム構成情報220が格納されている。

【0012】アクセス管理用サーバ300は、ディスクアレイ装置200におけるボリューム構成情報220の設定、スイッチ600を制御してデータアクセスのパスの制御などを行うことができる。具体的には、このアクセス管理用サーバ300は、メモリ230、メモリ302に格納されたプログラムを実行するCPU301、DB（データベース）部350を有している。またメモリ302には、ユーザ認証モジュール330、アクセス制御モジュール320、RAID構成管理モジュール310、スイッチ制御モジュール340といったプログラムが格納されている。

【0013】ユーザ認証モジュール330は、データアクセスホスト400や管理用クライアントコンピュータ500を通じてログインしたユーザの認証を行う。この認証に必要なユーザに関する情報（以下、単に「ユーザ情報370」と称する。）はDB部350より取得する。

【0014】アクセス制御モジュール320は、DB部350に格納されているアクセス権の情報（以下、単に「アクセス権情報380」と称する。）に基づき、ユーザのアクセスに対して許可あるいは不許可のいずれかの判断を行う。

【0015】RAID構成管理モジュール310は、ディスクアレイ装置200からボリューム構成情報220を取得し、定義したボリューム構成情報220をディスクアレイ装置200に設定する。

【0016】スイッチ制御モジュール340は、アクセス制御モジュール320が許可した場合に、論理ボリュームに対するデータアクセスが行えるようにする。具体的には、アクセス制御モジュール320の許可を受けて、スイッチ制御モジュール340は、パスを設定するためにスイッチ情報390をスイッチ600へ送る。

【0017】DB部350には、ディスクアレイ装置200のボリューム構成情報220によって定義された論理ボリュームの構成に関する情報（以下、単に「構成情報360」と称する。）が格納されている。さらに、このDB350は、前述したように、ユーザの認証に必要なユーザ情報370と、各論理ボリュームについて各ユ

ーザ毎に定義されたアクセス権情報380、スイッチのパスを設定するためのスイッチ情報390とが格納されている。

【0018】前述した構成情報の具体的な内容の一例について図2の構成情報を示すテーブルを参照して説明する。構成情報の項目としては、図2に示すように、各論理ボリュームの各ID（論理ボリュームID）に対し、それぞれ、ポートID（ポートアドレス）、LUN（Logical Unit Number）、デバイス番号（DEV、Logical Device Address）、ディスクアレイ装置のアドレス等が付与されている。論理ボリュームIDとは、データアクセスホスト（サーバ）400がアクセス可能な論理ボリューム（論理的なストレージボリューム）を示すIDである。ポートID、LUN、及びデバイス番号はデータアクセスホスト400のアクセスに用いる。そして管理対象となる全てのディスクアレイ装置に対してこれらの情報を管理している。

【0019】前述したユーザ情報370の具体的な内容の一例について、図3のユーザ情報を示すテーブルを参照して説明する。このユーザ情報の項目としては、図3に示すように、ユーザの各ID（ユーザID）に対し、それぞれ、ホストアドレス、パスワード、及び各ユーザの役割としてのアクセス権等が付与されている。ホストアドレスとは、ユーザが用いるデータアクセスホスト400に付与されている物理アドレス（World Wide Name）である。この物理アドレスは、一つのユーザIDに対し、複数定義可能である。例えば、図3のテーブルにおける一行目のユーザID“Na”に対し、二つのアドレス“01230”、“02345”、パスワード、アクセス権として“SSP（Storage Service Provider）管理権限”が定義されている。SSP管理権限とは、図3の説明の欄に記載されているように、SSPのリソースの全体（アクセス管理用サーバ300によって管理されるディスクアレイ装置200が有するすべての論理ボリューム）に対し、制限のないフルアクセスの権限が与えられていることを意味する。他のユーザIDも、図3のテーブルに記載された通りである。

【0020】前述したアクセス権情報380の具体的な内容の一例について、図4のアクセス権情報を示すアクセス管理テーブルを参照して説明する。このアクセス権情報の項目としては、図4に示すように、各ユーザに対し、それぞれ、各論理ボリュームについてのアクセス権情報（論理ボリューム実施設定権限情報を含む）が付与されている。

【0021】例えば、図4のテーブルの1列目のユーザID“Na”は、SSP管理者である。このため、ユーザID“Na”は、全てのストレージリソース（V01-0乃至V01-5）に対し、その構成の定義を参照（図中“R”）及び変更（図中“X”）する権限を有する。すなわち、ユーザID“Na”は、V01-0乃至V0

1-5について、論理ボリュームの定義の設定が許可とされる。一方、論理ボリュームのデータ自体に対する参照（読み出しや転送、図中“r”）及び書き込み（図中“w”）の権限は有しない（図中“—RX”）。すなわち、ユーザID“Na”は、V01-0乃至V01-5について、アクセス（データアクセス）が不許可とされる。

【0022】また、図4のテーブルの2列目のユーザID“Ha”は、A社が“A社aa”及び“A社ab”として割り当てられたストレージリソース（V01-0、V01-1）全体の管理者である。このため、ユーザID“Ha”は論理ボリュームV01-0、V01-1について、その構成の定義を参照（図中“R”）及び変更（図中“X”）する権限を有するとともに、論理ボリュームのデータ自体に対しても参照（図中“r”）及び書き込み（図中“w”）の権限を有する（図中“rwRX”）。すなわち、ユーザID“Ha”は、V01-0、V01-1について、アクセス（データアクセス）が許可とされる。また、このユーザID“Ha”は、自社たるA社以外の論理ボリューム（V01-2乃至V01-5）について参照、変更及び書き込みといった一切のアクセスはできない（図中“—”）。すなわち、ユーザID“Ha”は、V01-2乃至V01-5について、論理ボリュームの定義の設定が不許可とされる。

【0023】さらに、図4のテーブルの3列目のユーザID“Ka”は、A社のaa部門の管理者である。このため、ユーザID“Ka”は、aa部門に割り当てられた論理ボリュームV01-0についてのみ、その構成の定義を参照（図中“R”）及び変更（図中“X”）する権限を有するとともに、論理ボリュームのデータ自体に対しても参照（図中“r”）及び書き込み（図中“w”）の権限を有する（図中“rwRX”）。また、このユーザID“Ka”は、自部門社たるaa部門以外の論理ボリューム（V01-1乃至V01-5）について参照、変更及び書き込みといった一切のアクセスはできない（図中“—”）。

【0024】さらにまた、図4のテーブルの5列目のユーザID“Ue”は、A社のab部門の一般ユーザであり管理者ではない。このため、ユーザID“Ue”は、ab部門に割り当てられた論理ボリュームV01-1についてのみ、そのデータ自体に対しても参照（図中“r”）及び書き込み（図中“w”）の権限を有する一方、その構成の定義を参照及び変更する権限を有さない（図中“rw—”）。

【0025】前述したスイッチ情報390の具体的な内容の一例について、図5のスイッチ情報を示すスイッチ情報テーブルを参照して説明する。このスイッチ情報の項目としては、図5に示すように、スイッチのポート番号とゾーン定義情報が付与されている。

【0026】スイッチ600は、データアクセスホスト

400が論理ボリュームに対するデータアクセスを行えるようにするためにバスを設定する。具体的には、スイッチ600は制御部610を有し、アクセス管理用サーバ300から送られてくるスイッチ情報390に基づいてバスの設定を行う。つまり図5で示したスイッチ情報により同じゾーンが定義されたポート番号どうしを接続させる。例えば、PortAとPort Cとを接続させ、Port BとPort Dとを接続する。これにより、データアクセスホスト400と論理ボリュームとのバスが設定される。

【0027】（実施例）

<<第一実施例>> ユーザが、管理用クライアントコンピュータ500を用い、アクセス管理用サーバ300を介し、ディスクアレイ装置200のボリューム構成情報220を参照又は変更、すなわち設定を行う動作につき、図6の全体の処理、図7のフローチャート及び図1のブロック図を参照して説明する。なお、フローチャートを示す図面における“S”はステップを示す。

【0028】図6は、ユーザ情報370、アクセス権限380、ボリューム構成情報220の設定を行うための動作を示した図である。

【0029】ユーザは、管理用クライアントコンピュータ500を用いて他のユーザのアクセス権限を設定できる。具体的には、図3に示す「SSPのリソース全体へのファイルアクセス権限」を有しているユーザIDがNaのユーザは、ユーザIDがHaのユーザのアクセス権限を「A社割当てリソース全体へのファイルアクセス権限」と設定することができる。また、ユーザIDがHaのユーザは、A社割当てリソース全体に対して、ユーザIDがKa、Maのそれぞれのユーザのアクセス権限を設定することができる。このように、階層的にアクセス権を設定することができる。

【0030】まず、図3に示すユーザ情報に、ユーザID「Na」のアクセス権限が設定され、ユーザID「Ha」のアクセス権限を設定する場合について説明する。尚、以下の説明において「ユーザID「*」」とは、「ユーザ*」が利用するユーザIDである。

【0031】ユーザNaが管理用クライアントコンピュータ500へユーザID「Na」とパスワードを入力すると、管理用クライアント500の管理用UI510により、ユーザID、パスワードがアクセス管理用サーバ300へ送られる（601）。アクセス管理用サーバ300は、ユーザ認証モジュール330により認証を行い（602）、ユーザ情報に登録されているユーザID、パスワードと一致すると認証に成功したと判断し、アクセス制御モジュール320により、アクセス管理テーブルからユーザID「Na」が参照、変更できる論理ボリュームを特定する（603）。ユーザNaは、図4に示したアクセス管理テーブルよりv01-1～v01-5まで参照及び構成の変更ができるので、v01-1～v

01-5が特定される。特定された論理ボリュームに関する構成情報及びアクセス権限の情報はアクセス制御モジュール320により、管理用クライアントコンピュータ500へ送られる(604)。送られてきた構成情報は、管理用UI510により、管理用クライアントコンピュータ500の画面に表示される(605)。ユーザNaは、この画面を利用してユーザHaのアクセス権限を設定する(606)。

【0032】図8は、管理用クライアントコンピュータ500の画面表示例である。管理用クライアントコンピュータ500は、参照権限だけが与えられた論理ボリュームの構成情報が表示される領域801、参照及び構成の変更の権限が与えられた論理ボリュームの構成情報が表示される領域802、ユーザIDを設定する領域803、パスワードを設定する領域804、コメントを入力する領域805とが表示される。また画面には、アクセス権限を設定するためのボタンが表示されている。具体的には、構成情報の参照権限(R)を設定するボタン806、構成情報の変更権限(X)を設定するボタン807である。更に、設定されたアクセス権限を決定するための決定ボタン808、データアクセスホストと論理ボリュームとを定義するための画面に遷移するための定義ボタン809、処理を終了するための終了ボタン810が表示される。

【0033】図8に示すようにユーザNaは、ユーザHaのユーザIDとパスワードを設定する。次に、ユーザHaに割当する論理ボリュームを選択する。ここでは、マウス等を利用して対象とする論理ボリュームvol-0、vol-1を指定する。指定された論理ボリュームvol-0、vol-1は反転表示され、ユーザNaによって指定されたことが分かる。尚、指定できる論理ボリュームは、領域802に表示されたものだけであり、領域801に表示された論路ボリュームでも反転表示しない。次に、この指定された論理ボリュームに対するアクセス権限をマウス等で指定することで設定する。指定されたアクセス権限は、それぞれの論理ボリュームごとに表示される。また、ユーザNaは、ユーザHaのアクセス権限のコメントとして領域805に「A社全社管理権限：A社割当てリソース全体へのファイルアクセス権限」と入力する。全ての入力を確定すると、決定ボタン808を指定する。これにより、ユーザHaの構成定義情報に対するアクセス権限が設定された。

【0034】次に、定義ボタン809を指定すると図9に示すデータアクセスホストと論理ボリュームとを対応付けるための画面が表示される。この画面には、ホスト表示領域901、ボリューム構成情報表示領域902、データアクセスホストが登録されたファイルのファイル名を入力する領域903と決定のボタン904、データアクセスホストとボリュームとの定義を決定するボタン905、画面での処理を終了するボタン906とが表示

されている。更に、アクセス権限を設定するために、データの参照権限(r)を設定するボタン907、データの書き込み権限(x)を設定するボタン908とが表示されている。ボリューム構成情報表示領域902には、アクセス管理用サーバから送られてきたボリューム構成情報が表示されている。つまり、ユーザNaが設定することができる構成情報が表示される。また、ホスト表示領域901にアドレス、ユーザIDが表示されているが、これは、ユーザNaによって領域1003にファイル名が入力されて表示されたものである。尚、ユーザNaがキーボード等により、アドレス、ユーザIDを入力するようにしてもよい。ユーザNaがアドレスをマウス等で指定すると、指定されたアドレスが点滅する。この状態でユーザNaは、ボタン907、908を指定すると、データの参照権限(r)、データの書き込み権限(x)を設定することができる。他のアドレスを指定すると、点滅表示は反転表示に変わり、新たに指定されたアドレスが点滅する。このようにして、それぞれのアドレスに対して権限を設定する。次に、ユーザNaが論理ボリューム情報を指定すると、指定された論理ボリューム情報が反転表示となる。このように対応付けを行いたいアドレスと論理ボリュームとを反転表示にし、決定ボタン905を指定すると、反転表示されたアドレスと論理ボリュームとが対応付けられる。決定ボタン905を指定した後に、新たにアドレス又は論理ボリュームを指定すると、今まで反転表示されていたアドレス、論理ボリュームは元の表示状態に戻り、新たに指定されたものがアドレスであれば点滅し、論理ボリュームであれば反転表示となる。

【0035】ユーザNaが終了ボタン906を指示すると、図8の画面に戻り、更に終了ボタン810を指示すると、管理用UI510により設定された情報が登録情報としてアクセス管理用サーバ300へ送られる(607)。

【0036】アクセス管理用サーバ300では、アクセス制御モジュール320により、送られてきた登録情報をユーザ情報テーブル、アクセス権情報テーブルに登録する(608)。つまり、ユーザID、パスワード、コメントをユーザ情報370に登録し、ユーザID、アクセス権限をアクセス管理テーブルに登録する。これにより、ユーザHaは、論理ボリュームvol-1、vol-2に対して、構成定義の参照権限、変更権限、データの参照権限、書き込み権限が与えられ、ユーザHaは論理ボリュームvol-1、vol-2に対する他のユーザのアクセス権限を設定できるようになる。次に、RAID構成管理モジュール310により登録されたユーザ情報370、アクセス権情報380に基づいて構成情報を生成する(609)。図10は、生成された構成情報の一例を示したものである。また、RAID構成管理モジュール310は、生成された構成情報をディスクアレ

イ装置200へ送る(610)。

【0037】この設定により、ユーザHaが利用するデータアクセスホスト400からディスクアレイ装置にアクセスすることが可能になる。例えば、ユーザHaがデータアクセスホストからディスクアレイ装置200へデータを書き込む場合、データアクセスホスト400から論理ボリュームID、ホストのアドレス、書き込み命令、書き込むデータとをディスクアレイ装置200へ送る(611)。ディスクアレイ装置200では、送られてきた論理ボリュームID、ホストのアドレスとボリューム構成情報に登録された論理ボリュームID、ホストのアドレスとを比較し(612)、一致すれば、論理ボリュームIDに定義されたディスク装置へデータを書き込む(613)。

【0038】以上のようにしてユーザNaは、ユーザHaの論理ボリュームに対するアクセス権を設定することができる。

【0039】図7は、アクセス管理用サーバ300の処理を示したものである。

【0040】図7のフローチャートに示すように、処理開始後、ユーザが、管理用クライアントコンピュータ500の管理用UI510を実行して、アクセス管理用サーバ300にログインしてID等のユーザ情報を送信する。アクセス管理用サーバ300のユーザ認証モジュール310は、受け取ったユーザ情報に基づきDB部350のユーザ情報(図3)を参照し、ログインしたユーザの認証をおこなう(701)。認証に成功した場合(702: YES)、アクセス制御モジュール320が、DB部350のアクセス権情報(図4のアクセス管理テーブル)を参照して、認証されたユーザがアクセス可能な論理ボリュームを決定(許可)する(703)。次いで、RAID構成管理モジュール330は、S703で決定された論理ボリュームに関する構成情報(図2)をDB部350から取得し(704)、管理用クライアントコンピュータ500へ送る(705)。管理用クライアントコンピュータ500の管理用UI510は、送られてきた論理ボリュームに関する構成情報を画面に表示する。ユーザは、管理用UI510を通じ、表示された構成情報の論理ボリュームについて、その構成の変更(定義の設定)を行う操作を実行する。ユーザにより画面に表示されている「終了」が指示されると、管理用UI510は変更された論理ボリュームに関する構成情報をアクセス管理用サーバ300へ送る。

【0041】次に、送られてきた論理ボリュームに関する構成情報に従って、DB部350の構成情報を変更するとともにRAID構成管理モジュール310により、ディスクアレイ装置200へ変更された構成情報を送る(706)。ディスクアレイ装置200は、送られてきた構成情報をボリューム構成情報220としてメモリ230に格納する。ディスクアレイ装置200の制御部2

40は、変更されたボリューム構成情報220に従ってディスク装置210へのアクセスを制御する。

【0042】このように第1の実施例では、ボリューム構成情報の参照権限、変更権限の設定及び論理ボリュームに対するアクセス権限の設定について説明した。尚、図6ではボリューム構成情報の参照権限、変更権限と、論理ボリュームに対するアクセス権限とを設定する場合について説明したが、いずれか一方の設定だけを行うこともできる。そして、これにより構成情報の参照権限、変更権限を階層的に管理することができる。＜＜第二実施例＞＞ 第一実施例は、管理用クライアント500とアクセス管理サーバ300とを利用してディスクアレイ装置200のボリューム構成情報220を設定することについて説明した。第二の実施例は、これに加えてボリュームへのアクセス権限をデータアクセスホスト側で管理するようにしたものである。

【0043】具体的には、図6の処理608で生成されたユーザ情報370と、アクセス権情報380に基づいてデータアクセスホスト400ごとに論理ボリュームに対するアクセス権を特定する。例えば、図3に示すユーザ情報の中でホストアドレスが“02220”については、図11に示すような論理ボリュームに対するアクセス権限が生成される。このように生成されたアクセス制限情報を図6の処理610の後にホストアドレスに従って、それぞれのデータアクセスホスト400へアクセス制御モジュール320によって送る。送られてきたデータアクセスホスト400では、このアクセス制限情報をメモリ440に格納し、ディスクアレイ装置へアクセスするたびに、このアクセス制限情報に従って、ディスクアレイ装置へのアクセス権限を確認する。具体的には、データアクセスホスト400には、ディスクアレイ装置へのアクセスを制御するドライバが組み込まれている。このドライバは、アプリケーションから、論理ボリュームID、書き込み/読み出し命令、書き込み命令の場合は書き込むべきデータとを受け取って、FCIFを介してディスクアレイ装置に送っている。このドライバは、アクセス制限情報430が設定されると、アプリケーションから受け取った論理ボリュームIDと、書き込み/読み出し命令とがアクセス制限情報に登録されているかを確認する。登録されていないアクセスを許可し、登録されていないアクセスを拒否する。

【0044】このようにデータアクセスホスト側にアクセス制限情報を設定することでディスクアレイ装置に対して許可されないアクセスの発生を防止できるので、ネットワークの負荷を抑えることが可能となる。

【0045】尚、この実施例は、ユーザが別々のホストアドレスを利用することを前提としたものであり、別々のユーザが1つのデータアクセスホストを共有する場合には、ユーザIDとパスワードによって制限するようにすればよい。つまり、ユーザIDとパスワードでアクセ

ス制限情報を管理し、予め登録されたユーザID、パスワードが一致したら、このユーザIDに対して設定されているアクセス制限情報を利用すればよい。

【0046】<<第三実施例>> ユーザが、データアクセスホスト400を用い、アクセス管理用サーバ300を介し、ディスク装置210の論理ボリュームのデータにアクセスして参照又は書き込みを行う動作について図12のフローチャート及び図1のブロック図を参照して説明する。

【0047】ユーザは、データアクセスホスト400のホストエージェント410により、アクセス管理用サーバ300へ、ユーザのID、パスワード、ホストアドレスを送る。

【0048】図12のフローチャートに示すように、処理開始後、アクセス管理用サーバ300のユーザ認証モジュール330は、受け取ったユーザのID、パスワード、ホストアドレスに基づき、DB部350のユーザ情報(図3)を参照して、認証の処理を実行する(1201)。この認証が失敗した場合(1201:NO)、ユーザ認証モジュール330は、データアクセスホスト400にログインの失敗を通知する(1210)。反対に、この認証が成功した場合(1202:YES)、アクセス制御モジュール320が、DB部350のアクセス権情報(図4のアクセス管理テーブル)を参照し、認証されたユーザがアクセス可能な論理ボリュームの情報を検索する。(1203)。図4に示したユーザID“Ha”の場合は、検索した結果V01-0、V01-1となる。つまり、ユーザID“Ha”の場合は図4より“r”または“w”が定義されているのはV01-0、V01-1だからである。次に、検索された論理ボリュームの情報を当該ユーザのホストアドレスとともにディスクアレイ装置200へ送る(1204)。

【0049】ディスクアレイ装置200では、送られてきた論理ボリューム情報により、ホストアドレスをボリューム構成情報220に登録する。例えば、論理ボリューム情報“V01-0”、“V01-1”、ホストアドレス“02220”が送られてきた場合のボリューム構成情報220は図10のようになる。このように“V01-0”、“V01-1”に対してホストアドレスが設定される。ディスクアレイ装置200の制御部240は、ファイバチャネルを経由して送られてきたホストアドレスがボリューム構成情報220の当該論理ボリュームに登録されているか、当該アクセスが有効であると判断し、アクセスを許可する。ホストアドレスが登録されていない場合は、アクセス失敗の通知を送る。

【0050】再び図12に戻って説明を続ける。ステップ400でディスクアレイ装置へ論理ボリュームの情報を送った後に、アクセス制御モジュール320は、スイッチ制御モジュール340へ指示を出す。スイッチ制御モジュール340は、スイッチ情報390をスイッチ6

00へ送る(1205)。ここで、スイッチ600の制御部610は、スイッチ情報390により設定が終了すると、パス設定が成功したことアクセス管理用サーバ300へ送る。アクセス制御モジュール320は、パス設定が成功した通知を受けると、パス設定完了をデータアクセスホスト400へ送る(1207)。データアクセスホスト400は、パス設定完了通知を受けて、ディスクアレイ装置200へのデータアクセスを開始する。

【0051】アクセス制御モジュール320は、データアクセスホスト400からログアウトの通知を受けると(1208:YES)、スイッチ制御モジュール340に対してスイッチの解除を指示する。スイッチ制御モジュール340は、解除通知をスイッチ600へ送る(1209)。スイッチ600の制御部610は、解除通知を受けて設定を解除する。

【0052】このように、本実施例ではディスクアレイ装置のボリューム構成情報とスイッチの設定による、ユーザのアクセス管理の方法を示した。

【0053】尚、図1に示したシステムでスイッチがないシステムまたはスイッチのパスが既に設定されている場合であっても、本発明を適用することができる。ただし、その場合には図12に示した処理の中で処理1205-処理1207の処理がなくてもよい。

【0054】<<第四実施例>> ユーザが、データアクセスホスト400を用い、アクセス管理用サーバ300を介し、ディスク装置210の論理ボリュームのデータにアクセスして参照又は書き込みを行う他の動作について図13のフローチャート及び図1のブロック図を参照して説明する。ユーザは、データアクセスホスト400のホストエージェント410により、アクセス管理用サーバ300へ、ユーザのID、パスワード、ホストアドレスを送る。

【0055】図13のフローチャートに示すように、処理開始後、アクセス管理用サーバ300のユーザ認証モジュール330は、受け取ったユーザのID、パスワード、ホストアドレスに基づき、DB部350のユーザ情報(図3)を参照して、認証の処理を実行する(1301)。この認証が失敗した場合(1302:NG)、ユーザ認証モジュール330は、データアクセスホスト400にログインの失敗を通知する(1305)。反対に、この認証が成功した場合(1302:YES)、アクセス制御モジュール320が、DB部350のアクセス権情報(図4のアクセス管理テーブル)を参照し、アクセス可能な論理ボリュームと、その権限が定義されたアクセス制限情報を生成する(1303)。図4に示したユーザID“Ha”の場合は、既に説明したように図11に示すようなものとなる。アクセス制御モジュール320は、図11に示した論理ボリュームとその権限が定義されたアクセス制限情報を、データアクセスホスト400へ送る(1304)。

【0056】データアクセスホスト400は、送られてきたアクセス制限情報420をメモリへ格納する。データアクセスホスト400は、ディスクアレイ装置200へアクセスするためのアプリケーション、ドライバなどのプログラムがメモリに格納されている。ユーザからの要求でディスクアレイ装置200へのアクセスが発生すると、メモリに格納されたI/Oドライバプログラムの実行によりアクセス情報420を参照し、アクセス要求の対象となったボリュームへのアクセス権限はあるか、また当該要求（参照、書き込み）の権限があるかを判断する。当該要求を満たす権限がある場合には、ディスクアレイ装置200に対して、ホストアドレスを送り、アクセスを実行する。一方、当該要求を満たす権限がない場合には、権限がない旨を画面に表示する。

【0057】以上説明したように、本実施例はユーザのボリュームに対するアクセス権限をアクセス管理用サーバ300で生成し、通知することで、ユーザが利用するデータアクセスホスト400により制御できるようにしている。

【0058】尚、スイッチ600の制御も含むようにする場合、図12に示した処理1206—処理1207までの処理を図13の処理1307の後に行うようにすればよい。

【0059】以上、本発明について、実施の形態に基づき具体的に説明したが、これに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。また、本実施の形態によれば、ユーザ毎に論理ボリューム単位でアクセスの制御を行うことができる。例えば、ユーザのタスク（役割）に応じたアクセス制御を実現できる。

【0060】

【発明の効果】論理ボリューム単位でアクセスの制御を行うことができる。

【図面の簡単な説明】

【図1】ストレージシステムを含む全体構成を示すブロック図である。

【図2】ディスクアレイ装置が備える論理ボリューム

の構成情報の一例に関するテーブルを示す図表である。

【図3】ディスクアレイ装置が備えるユーザ情報の一例のテーブルを示す図表である。

【図4】ディスクアレイ装置が備えるアクセス権情報の一例を示すアクセス管理テーブルを示す図表である。

【図5】アクセス管理方法で用いられるスイッチ情報の一例を示すテーブルを示す図表である。

【図6】システム全体の動作を示した図である。

【図7】アクセス管理方法の第一実施例を示すフローチャートである。

【図8】論理ボリュームに対する構成変更の定義を行う画面の一例を示した図である。

【図9】論理ボリュームに対するアクセス権を設定する画面の一例を示した図である。

【図10】アクセス管理方法で用いられるボリューム構成情報を示す図表である。

【図11】論理ボリュームとその権限とが定義されたアクセス制限情報を示す図表である。

【図12】アクセス管理方法の第二実施例を示すフローチャートである。

【図13】アクセス管理方法の第三実施例を示すフローチャートである。

【符号の説明】

- 100 ディスクアレイシステム
- 200 ディスクアレイ装置
- 210 ディスク装置
- 220 論理構成制御部
- 300 アクセス管理用サーバ
- 310 ユーザ認証部
- 320 アクセス制御部
- 330 RAID構成管理部
- 340 バス制御部
- 350 DB部
- 400 データアクセスホスト
- 410 ホストエージェント部
- 500 管理用クライアントコンピュータ
- 510 管理用UI部

【図2】

図2

論理ボリュームID	ポートID	LUN	アクセス権付 (CSP/200)	ディスクアレイ装置 アドレス
Vol-0	CL0-A	0	01FC	0001
Vol-1	CL0-A	1	01FF	0001
Vol-2	CL0-B	0	0200	0001
Vol-3	CL0-A	1	020C	0001
Vol-4	CL0-B	0	0240	0002
Vol-5	CL0-A	1	0240	0002

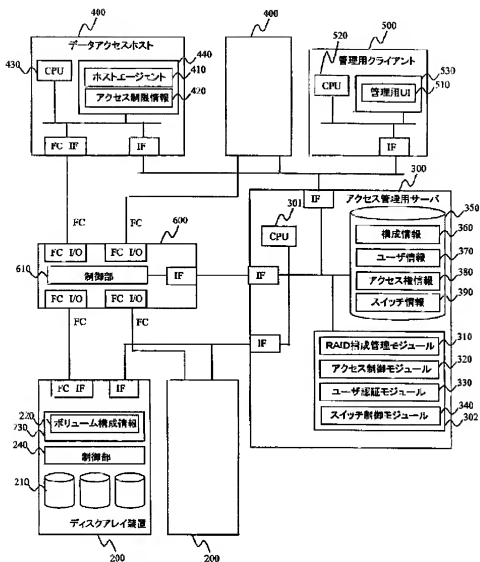
【図5】

図5

ポート	ゾーン番号
Port_A	ゾーン1
Port_B	ゾーン2
Port_C	ゾーン1
Port_D	ゾーン2

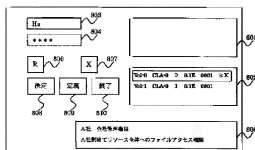
【図1】

【図1】



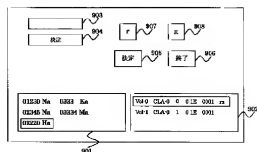
【図8】

図8



【図9】

図9



【図3】

【図4】

【図5】

ユーザ情報

ユーザID	ホストアドレス	パスワード	所属	説明
He	01130	*	S&I*	S&Iのリソース全体へのフルアクセス権限
He	0209	*	A社	A社側でリソース全体へのフルアクセス権限
Ke	0209	*	A社	A社のab部門のリソースへのフルアクセス権限
Ma	03334	*	A社	A社のab部門のリソースへのフルアクセス権限
Ue	03370	*	A社	A社のab部門の一般ユーザアクセス権限
He	06506	*	B社	B社側で全リソースへのフルアクセス権限
Ta	03589	*	B社	B社のba/ba部門のリソースへのフルアクセス権限
Ok	03581	*	B社	B社のba/ba部門のリソースへのフルアクセス権限
Re	03581	*	B社	B社のba/ba部門の一般ユーザアクセス権限
Ke	03586	*	B社	B社のba/ba部門の一般ユーザアクセス権限
On	92000	*	B社	B社のba/ba部門の一般ユーザアクセス権限

【図6】

アクセス権限テーブル

	権限ポリシー					
	Val-0	Val-1	Val-2	Val-3	Val-4	Val-5
He	-RX	-RX	-RX	-RX	-RX	-RX
He	rwRX	rwRX	---	---	---	---
Ke	rwRX	---	---	---	---	---
Ma	---	rwRX	---	---	---	---
Ue	---	rw	---	---	---	---
He	---	---	rwRX	rwRX	rwRX	---
Te	---	---	rwRX	rwRX	---	---
Ok	---	---	---	---	---	---
Ke	---	---	rw	---	---	---
Ba	---	---	---	rwRX	---	---
Sh	---	---	---	---	rw	---
	A社	A社	B社	B社	B社	B社

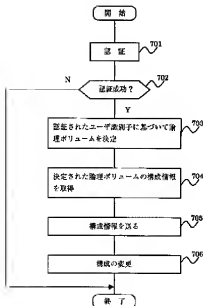
凡例: r(データの参照権限), w(データの書き込み権限), R(読取情報の参照権限), X(読取情報の書き込み権限), --- (権限無し)

【図7】

【図10】

図 7

図 10



【図11】

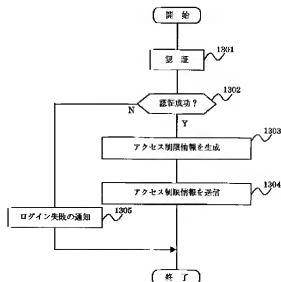
【図12】

権限ポリシーID	権限
Val-0	---
Val-1	rw

権限ポリシーID	ポートID	URL	デバイス番号 (OU Level)	ホストアドレス
Val-0	010-A	0	010	000000
Val-1	010-A	1	010	000000
Val-2	010-B	0	010	000000
Val-3	010-B	1	010	000000
Val-4	010-B	0	140	000000
Val-5	010-A	1	140	000000

【図13】

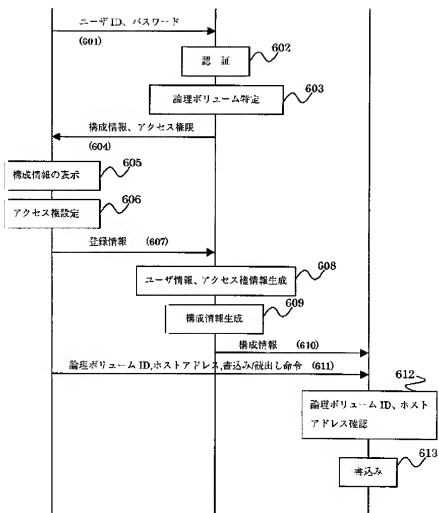
図 13



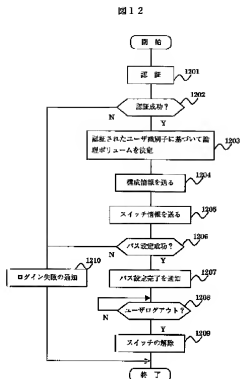
【図6】

図 6

管理用クライアント アクセス管理サーバ ディスクアレイ装置
コンピュータ



【図12】



フロントページの続き

(72)発明者 園村 智弘
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア事業部内
(72)発明者 河野 敏彦
神奈川県横浜市戸塚区戸塚町5030番地 株
式会社日立製作所ソフトウェア事業部内

(72)発明者 篠原 大輔
神奈川県川崎市麻生区王禅寺1099番地 株
式会社日立製作所システム開発研究所内
Fターム(参考) 5B065 BA01 CA30 CC03 PA02 PA04
PA12